

FEDERAL BUREAU OF INVESTIGATION
FOI/PA
DELETED PAGE INFORMATION SHEET
FOI/PA# 1498459-000

Total Deleted Page(s) = 3
Page 4 ~ Duplicate;
Page 5 ~ Duplicate;
Page 6 ~ Duplicate;

XXXXXXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X For this Page X
XXXXXXXXXXXXXXXXXXXXX

b3
b6
b7C
b7EContinuation of FD-302 of , On 08/04/2010, Page 3

access and knowledge of CHOICE ADVANTAGE, and could have had access indirectly to the encryption keys and would have had knowledge of the standard Intrusion Detection System (IDS) rule set. believes is still in the Phoenix area and is working for a police department.

b6
b7C

After a briefing by the interviewing agent regarding cyber security and issues other financial institutions and government contractors have faced, the group remembered an incident that occurred between September 2008 and July 2009 where some individuals were calling franchisee hotels advising they were with the CHOICE ADVANTAGE role out team and they were needing them to go to a specific web page and download updates to their system. believes the Phoenix Division of the FBI was able to identify the perpetrators and it turned out to be some teenagers. They were not aware of the status of the case.

b6
b7C

Choice has been consulting with remediation companies with experience in the hospitality industry as an effort to secure their network further. They do not believe their entire network is compromised at this time because keeps communicating with them via e-mail. Despite the fact the e-mails have escalated from advising them of the situation, to asking for a job, to wanting a consulting agreement paid through Western Union to his latest e-mail stating he is planning on stopping all communication, stealing the data, and selling it on the black market.

b6
b7C

Continuation of FD-302 of [REDACTED]

, On 08/04/2010 , Page 2

[REDACTED]

resolve the problem as well as offered to provide proof of the breach. Follow-up e-mails with [REDACTED] indicated the intruder did indeed have access to credit card data and Choice verified that data was indeed accurate.

[REDACTED] stated based upon the data accessed by [REDACTED] it was discovered he had used a compromised generic login titled

[REDACTED]

Since the incident, Choice has changed the password on the account, turned on all possible logging on the account and has been monitoring access from that IP Address as well as access from IP Addresses from [REDACTED] further advised the

[REDACTED]

At this point there is no specific individual or any other threat that has occurred recently to tie this incident with anyone currently or formerly employed. However, there was a fairly recent termination from the Information Security Department that does raise a question. An employee by the name of:

DOB: [REDACTED]

SSAN: [REDACTED]

[REDACTED]

was terminated from Choice on [REDACTED] who had [REDACTED] terminated, stated [REDACTED] lacked both technical expertise and motivation to do the job he was hired to do. However, he did have

b3
b6
b7C
b7Eb6
b7C
b7Eb6
b7C
b7Eb6
b7C

- 1 -

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 08/05/2010

[redacted] for Choice Hotels International, and [redacted] for Choice Hotels International (Choice), were interviewed at the corporate offices of Choice Hotels at 10750 Columbia Pike, Silver Spring, MD 20901. On the phone and participating from Choice's datacenter in Phoenix, Arizona, was [redacted]. After being advised of the nature of the interview and the identities of the interviewing agents, [redacted] provided the following information:

b6
b7C

Choice has been in the process of converting all franchisee hotels to a central system known as CHOICE ADVANTAGE. This system would allow for central processing of reservations, occupancy and billing information for all guests of all properties currently on the system. Authorized users could log into the system from anywhere on the Internet and conduct business. Typically most access was being conducted from the individual properties, however, since 99% of all the Choice properties are independently owned and operated, it is known that typical access does not necessarily come directly from the properties. In many cases the owners or managers are accessing the system from their homes, offices off the franchisee's property, or from laptops while traveling.

Handwritten: *Study*
1/2
JD

The CHOICE ADVANTAGE has been rolled out to over 3,000 properties world wide and has replaced an older system. The older system was an unconsolidated system which required a managed server be located on each property. From a risk perspective, Choice executives thought the older system was more vulnerable since the servers were not necessarily isolated and secured.

On July 13, 2010, an e-mail was received from [redacted] stating the individual had recently stayed at a hotel and was concerned about how easily they were able to get into the hotel's system and access hotel data. In particular, the individual was able to access personally identifying information (PII) of guests, to include name, address, e-mail address, credit card number, expiration date, telephone number, and other information collected from reservations and check-in. The sender of the e-mails identified himself as [redacted] and offered to help them

b6
b7CInvestigation on 08/04/2010 at Silver Spring, Maryland*See A3*File # [redacted] Date dictated Not Dictatedby SA [redacted] :ejob3
b6
b7C
b7E

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

Handwritten: *8/6/10*